

n° 148

high availability electrical power distribution

Guy Gatine

**Merlin Gerin engineer since 1982.
In 1965, in charge of research on means of testing semi-conductors for the Radiotechnique company.
In 1966, he became a research manager in the Merlin Gerin automation branch, and then worked in the SES (Electronic Safety Systems) department.
Presently, still in the SES department, and enriched by his long-standing experience in the nuclear and military fields, he directs the consulting and design of high level quality and availability installations.**

E/CT 148 first published october 1991

glossary

■ **ASEFA**, French Equipment Testing Station Association, part of the RNE: National Testing Network.

■ **LCIE**, Central Electronics Industry Laboratory.

■ **MDT**, Mean Down Time: mean failure duration.

■ **MTBF**, Mean Time Between Failures: mean operation time of a device in between two failures.

■ **MTTF or MTFF**, Mean Time to First Failure: mean proper operation time before the first failure occurs.

■ **UPS**, Uninterruptible Power Supply: comprising a battery charger, battery and inverter.

high availability electrical power distribution

The objective of this «Cahier Technique» is to explain to electrical installation designers how to design electrical power distribution systems that fulfil the objective of continuous voltage supply across the feeder terminals.

In other words: how to master power availability so as to achieve: "**the operating DEPENDABILITY objective**".

contents

1. Introduction		p. 4
2. Designing a dependability system		p. 4
	Specifying	p. 5
	Constructing	p. 5
	Demonstrating	p. 6
3. Description of a "backed-up" installation	Distribution circuits	p. 7
	Diesel generator set	p. 7
	Power source changeover devices	p. 8
	"Short-term" back-up	p. 8
	Electronic control-monitoring system	p. 8
	Operating criteria	p. 8
	Search for and identification of weak points	p. 9
4. Solutions for increasing availability	Knowing the level of component reliability	p. 9
	Choosing technologies	p. 10
	Failure tolerance	p. 12
	Running the installation	p. 13
5. Example of increased availability backed-up distribution	Specification	p. 16
	Construction	p. 16
	Maintenance arrangements	p. 17
	Demonstrating specified availability	p. 17
6. Conclusion		p. 18
7. Bibliography		p. 19

1. introduction

Operating dependability is a **fundamental characteristic** of all systems, installations and products. It is determined by **design** and **use**.

Dependability describes the aptitude of a system to «operate properly» throughout its service life. Proper operation implies:
- not breaking down (reliability),
- not experiencing dangerous failures (safety),
- being in good operating condition as often as possible (availability),
- being quickly repairable (maintainability).

Whatever the system and the efforts implemented in its design and use, the level of dependability is a concrete reality. It must be:
- taken into account starting at the design phase,
- observed a posteriori: by counting the operating hazards that occur during installation operation.

Electricity, a modern source of energy, contributes to the level of dependability through the fact that it is needed for operation. Its availability, or rather its unavailability, has increasingly important consequences on companies' competitiveness:
- **in industry**,
lack of power causes production losses,
- **in the service sector**,
lack of power causes computer blockages and utility shutdowns (lighting, heating, lifts...).

The more complex the systems, the higher the risk that even a brief power failure will have major consequences.

Safety and **availability** have been particularly well developed and mastered in previous years in fields such as nuclear, military and space. Nowadays, energy availability is a definite concern with regard to intelligence, monitoring of the most widely varied systems and, to an increasing extent, with regard to the power supply of those same systems.

Electrical power installations, especially those containing sensitive feeders, must be designed so as to limit the occurrence and consequences of failures in the public distribution network (referred hereafter in the booklet as the «mains»).

2. designing a dependability system

Beginning with a **simple, minimal system**, the design approach that has been adopted highlights the **strong points** and **weak points** of an electrical supply system, sometimes called a power station.

The weak points are then reinforced:
- **increased sturdiness and quality** of constituents,
- **redundancy** of equipment (duplication, «triplication»...).

The design is therefore **optimized** with a view to achieving the required level of dependability: the effort employed in design concern only the weak points of the system.

This approach necessitates the use of a rigourous design **methodology** together with dependability **techniques**.

The design phase (cf. fig. 1) takes place in three stages:

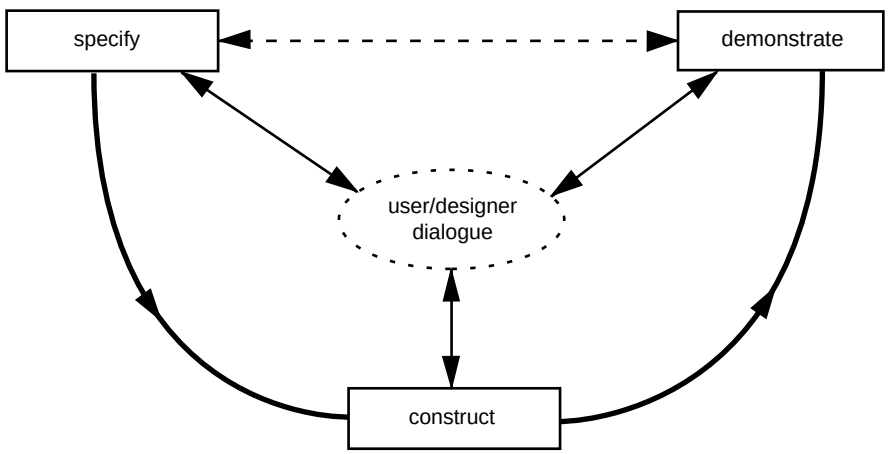


fig. 1: design method.

■ specifying,
■ designing/constructing,
■ demonstrating.

The dependability of a system, based on specifications, is well illustrated by the very definition of dependability as used by task forces specialized in operating dependability, IFIP at the world level and EWICS at the European level:
the **Quality of the service** supplied is such that the user has **justified confidence** in it.

The design of a dependability system therefore requires that the expected service be **specified** (knowing the need), that this service be **constructed** (quality of design), and that it be **demonstrated** that the solution complies with the dependability specification (justified confidence).

specifying

Specification of dependability constraints enables the «target» to be identified and the right amount of effort to then be devoted to design.
This stage has a decisive effect on the system.

Specification can be based on:
■ the **history** of «malfunctions» in similar installations (existing power stations),
■ **standards** (e.g. MIL) or recommendations,
■ **economic analyses** establishing the cost of installation down time (direct and indirect consequences) as a result of failures,
■ identification of the most dreaded events.

Dependability is a generic concept encompassing four criteria:
■ reliability,
■ safety,
■ availability,
■ maintainability.
Cahier Technique n° 144 «Introduction to dependability design» gives, among other things, a precise, official definition of these terms.

Using these criteria, the «specifier» establishes the dependability characteristics for his installation, based on these four criteria which are naturally quantifiable.
Through dialogue with the customer, the most dreaded events are determined, together with the acceptable probability of the occurrence of such events according to the seriousness of the consequences thereof.

constructing

Once the dependability objectives have been established, the dependability system («how to prevent the occurrence of failures» and how to master them) is «constructed». The means of doing so are listed below.

■ **quality: a dependability system is above all a quality system (failure avoidance)**
Quality must be taken into account at two levels:
□ quality of **design**, so as to guard against design errors (project team, quality assurance manual, audits...),
□ quality of **constituents**, so as to guard against failures (sturdiness, qualification).
■ **surviving failures (**failure tolerance)
The sturdiness and quality of the system are not sufficient criteria to guarantee its dependability. Certain functions are critical with respect to the assignment to be accomplished: the failure of a single component can bring about a loss of the power supply.
The system must therefore be designed so as to respect dependability objectives in spite of the failures that may occur, this being generally achieved through redundancy or the use of special technology (example: failure-oriented logic in electronics).

In order to survive failures, it is essential to **detect** the faulty function.
It is then necessary to:
□ **orient the failures** so that they do not affect the assignment (technological barriers), and then
□ **mask the failures** through the parallel operation of several units (even though only one would suffice), thereby enabling operation to continue with equivalent (standby) equipment.

In order to employ the right amount of effort in terms of failure avoidance and/or failure tolerance, measurements or calculations of the efficiency of such arrangements are carried out to directly evaluate the design and adapt the system architecture to best fit the cost.

This approach is «constructive»: the initial architecture is the simplest possible, minimal one (only «relevant» functions are taken into account); the architecture is then enriched according

to the results of the dependability evaluation so as to attain the target set during the specification stage.

Two iterations, implementing the study phases described in figure n° 2, are generally needed to design a system to the dependability requirements.

■ the first iteration consists of:

□ consolidating the dependability requirements,

□ establishing by means of a functional analysis method the simplest possible, minimal initial architecture,

□ evaluating the degree of dependability of this architecture,

□ proposing a certain number of corrective measures relative to the design so as to comply with the dependability requirements.

■ the purpose of the second iteration is to:

□ reassess the level of dependability of the «corrected» architecture,

□ conclude (or not conclude, in which case the process needs to be reiterated) upon the validity of the architecture with respect to the dependability objectives.

demonstrating

In order to achieve justified confidence, the customer must be given proof that the dependability level complies with the specified objective.
This is done by means of two techniques:

■ elimination of design-related failures: debugging, tests, environmental testing...

■ prediction of failures so as to measure the risk (probability) incurred during the system operating life.

Breakdown prediction involves dependability studies which, through modelling and evaluation, estimate the presence, creation and consequences of failures.

Predictive dependability studies are carried out using a set of modelling methods (FMECA - Failure Modes Effects and Critically Analysis method, failure tree, Markov graph…).

Quantitative evaluation is based on analysis of similar equipment having experienced problems in industrial operation and/or on the results of analyses recorded in reliability reviews (CNET, IEEE...).

Dependability studies make it possible to achieve «justified confidence» in the installation.

In the simplest electrical power distribution diagram, with power from the mains (cf. fig. 3), the level of availability of one of the feeders cannot be higher than the network level.

Considering that a mains failure incorporates the following criteria:

■ out-of-range voltage,

■ phase loss,

■ harmonic distortion (in the case of power supply for sensitive systems such as electronic systems).

The average level of unavailability of the French Electricity Board (EDF) mains is in the vicinity of a cumulative total of 7 to 8 hours per year (i.e. an unavailability rate in the range of 10^{-2} according to TDF observations), essentially due to the environment (e.g. storms).

It is therefore evident that if one wishes (specification) to improve the level of unavailability, to 10^{-4} for instance, it is necessary to provide for an architecture that is more than a mere radial feeder system, and more like an improvement on the basic diagram as illustrated in figure n° 4.

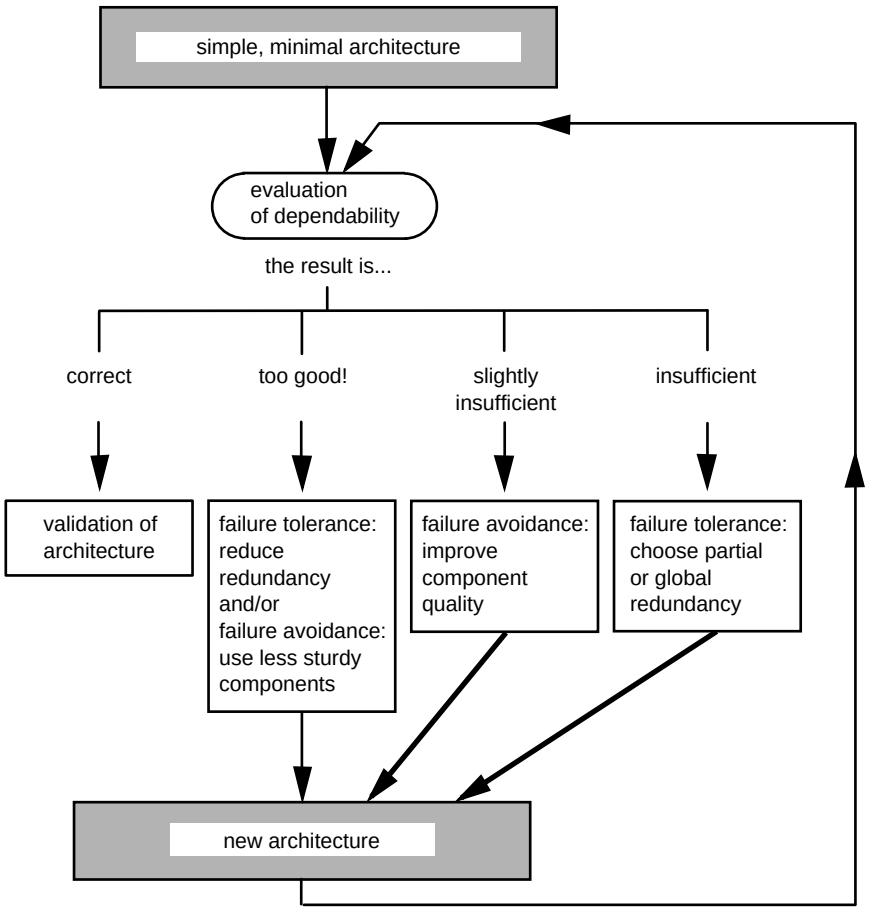


fig. 2: approach to employ the right amount of effort to dependability.

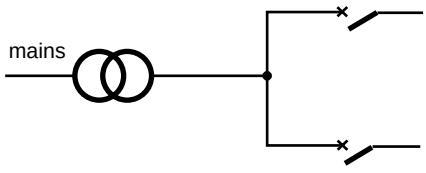


fig. 3: energy availability on one feeder cannot be higher than that of the source.

3. description of a «backed-up» installation

distribution circuits

(cf. fig. 4)

These circuits comprise essentially:
■ in Medium Voltage:
□ protection for the Medium Voltage (MV) incoming feeder,
□ MV/LV transformer;
■ in Low Voltage:
□ a main circuit breaker that protects the switchboard as a whole and eliminates the risk of inadvertent connection of the diesel generator set to the mains,
□ equipment for the protection of people and property against insulation faults;
■ feeder group power circuit breakers that distribute power, these breakers:
□ opening each time there is a power source changeover,
□ closing simultaneously if supplied by the mains,
□ closing in sequence if supplied with back-up power by the generator;
■ a power source changeover (mains/ generator) controlled by the mains/ standby voltage monitoring relay;
■ power source changeover that switches to the short time back-up source (UPS), generally a static contactor.

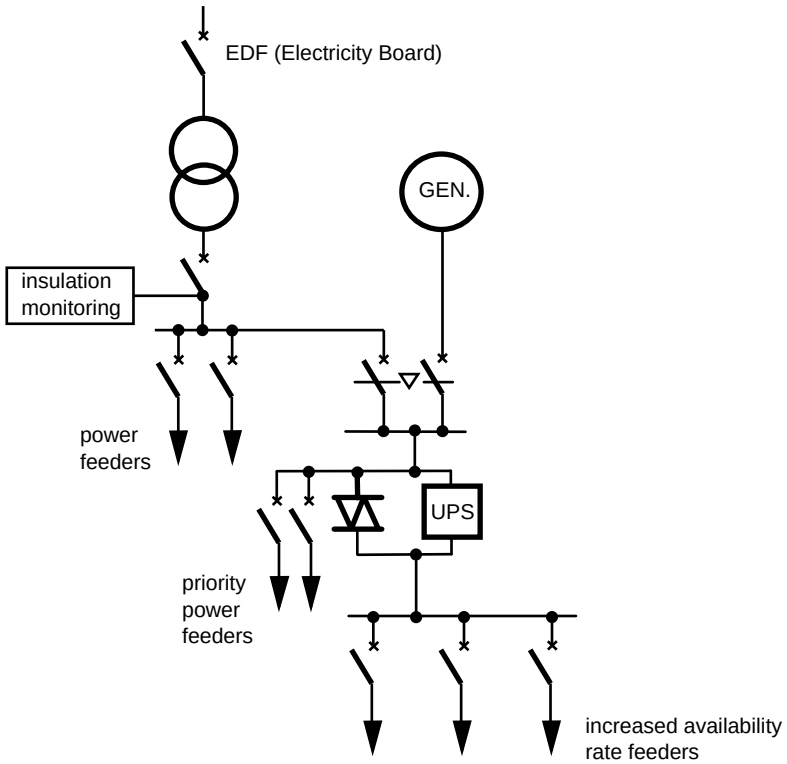


fig. 4: schematic diagram of «backed-up» electrical power distribution.

diesel generator set

(cf. fig. 5)

This equipment includes:
■ a diesel power motor suited to the power needs of the application.
It is equipped with auxiliary circuits:
□ a starting circuit including one or two starting chains (cf. chap. 4 § «choosing technologies»); each comprising a starter and a battery with a charger;
□ a gas oil circuit including:
- a so-called «daily» tank, with a maximum capacity of about 500 litres (depending on the generator power rating),
- an outside tank with a capacity calculated according to the maximum required motor autonomy,

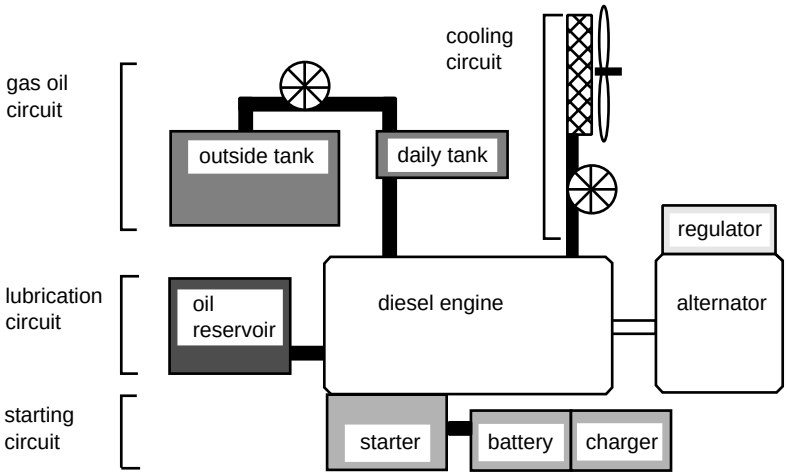


fig. 5: description of a diesel generator set.

- an automatic gas oil pump backed by a hand pump enabling the daily tank to be filled from the outside tank. This pump is not necessary if the daily tank is installed above the motor at a height calculated according to the pressure imposed by the injection circuit;
□ a pre-lubrication and lubrication circuit fitted with an oil reservoir calculated according to the motor autonomy chosen in order to fulfil special Electricity Board peak consumption compensation tariff requirements;
□ an air or water cooling circuit depending on the type of motor.
In the case of air-cooled generators, the motor is cooled by a fan driven by the motor shaft, either directly or by belts.
In the case of water-cooled motors, the inclusion of an exchanger (primary and secondary circuit) and an air cooler entail the use of circulation pumps and a fan.

■ a power alternator suited to the need, fitted with a voltage regulator.
The alternator reactance rates should comply with the type of load (reactive, capacitive, electronic system...).
For example, an application comprising 50 % of the load in the form of uncoupling battery rectifier-chargers entails the use of an alternator with a subtransient reactance rate of about 8 % in order to limit voltage distortions.

power source changeover devices

These devices make it possible to «switch to» the diesel generator set.

Aside from mains losses, switching or coupling can prove to be necessary in the two following cases:
■ failure of the «short-term» back-up source with the mains on,
■ detection of a mains anomaly (frequency, wave form, out-of-range rms value).

In both cases, temporary coupling to the mains prevents power cuts due to generator takeover time.

«short-term» back-up (UPS)

This function, comprising the «Uninterrupted Power Supply» (UPS), is fulfilled by one or more UPS with unit power of 40 to 800 kVA or more, equipped with a control-monitoring device, a battery and a diagnostic device that communicates via an asynchronous link. These types of UPS can be installed in parallel.
Battery autonomy should be sufficient (cf. table in figure n° 6) to supply power to the application during the time required for the generator to takeover as the long term back-up source. This takeover sequence includes:
■ mains actually out : 20 s
■ generator starting taking into account a startup at the last attempt : 50 s
■ Mains/Standby changeover (load shedding, then changeover) : 20 s
■ restoring of priority circuit breakers : 210 s

for a total sequence time of 5 minutes (100 s for the highest priority feeder).

electronic control-monitoring system

This system is a federation of electronic control or monitoring units (CU), each of which runs one of the main installation constituents (generator, source changeover,...).

These CU are combined with one or more supervision units (SU) which enable man-process dialogue but do not play a direct active role in the system.

operating criteria

A distribution system of this type, with a service life of 20 years for example, should ensure the electrical power supply when the following mains faults occur:
■ mains loss,
■ out-of-range mains voltage,
■ out-of-range phase unbalance.

Furthermore, it should also fulfil utility tariff constraints such as:
■ peak consumption compensation,
■ additional power beyond subscribed power.

The operation of each item of equipment comprising the station is linked to its role in the station and is defined as follows:
■ out-of-range mains voltage,
□ the diesel generator set operates as follows:
- mains failure : 200 h/y
- tariff constraints : 400 h/y
- testing : 50 h/y

i.e. maximum cumulative operation total : 650 h/y

□ the low voltage switchboard operates as follows:
- standby position : 8 % of the time
- mains position : 92 % of the time

■ the «short-term» back-up source takes over:
□ during very brief power cuts (micro-cuts) that vary in number depending on the power supply network and the environment,
□ during the phase in which the diesel generator set takes over the power supply, to which must be added low voltage switchboard switching times. 10 minutes' autonomy is ordinarily required of batteries at the end of their service life, 5 minutes being the minimum,
□ during battery test cycles. Very brief in duration, these are negligible in relation to the takeover phases.

Maintenance time should be provided for.
The selected availability guarantee is also linked to repair time. These times and the related means depend on the chosen level of dependability.

battery autonomy (mn)				
at the end of battery life	10	10	7	5
at the beginning of battery life	15	15	10	8
target unavailability levels for the installation as a whole:	**10^{-6}**	**5.10^{-6}**	**10^{-5}**	**10^{-4}**

fig. 6: UPS battery autonomy according to unavailability level.

search for and identification of weak points

The minimal basic architecture is analyzed, taking into account:
■ feedback on experience from various sources,
■ failure rates established by manufacturers and standardization bodies such as IEEE, MIL and CNET which allow the weak points of this type of installation to be established.
The failure probabilities for the main constituents of the installation, expressed in terms of the number of minutes of failure per year, are for example:

■ MV mains	=	450 mn/y,
■ LV switchboard	=	90 mn/y,
■ diesel generator set	=	360 mn/y,
■ short-term back-up	=	150 mn/y.

The «weights» that the components of each of the above bear on unavailability are as follows:

■ main low voltage switchboard

□ power source changeover	:	65 %
□ distribution equipment	:	25 %
□ auxiliary and control-monitoring	:	10 %
		100 %

■ diesel generator set

□ starting chain	:	65 %
□ cooling circuit	:	8 %
□ fuel circuit (gas oil pump)	:	7 %
□ generator load takeover	:	6 %
□ generator environment (e.g. temperature)	:	6 %
□ auxiliaries + control-monitoring	:	8 %
		100 %

■ short-term back-up

□ rectifier and frequency converter	:	35 %
□ batteries	:	55 %
□ auxiliaries	:	10 %
		100 %

It is easy to observe that the three «sensitive constituents» are:
■ the LV switchboard power source changeover,
■ the generator starting chain,
■ the short-term back-up battery.

4. solutions for increasing availability

The minimal basic architecture (cf. fig. 4) studied above, produces a maximum unavailability rate of about 5 h per year (i.e. 6.10^{-4}) with minimal back-up battery autonomy of 10 mn, and preventive and corrective maintenance requiring no assistance (cf. fig. 12).

The distribution of failure probabilities is expressed in terms of minutes of «failure» per year. If the targeted unavailability is less than 1 h/y (10^{-4}) on the feeder backed up by the UPS, improvements need to be made to the basic architecture and/or components. This is possible by:
■ ensuring key component reliability;
■ choosing the appropriate technologies and techniques;
■ having a fine division of operation in the aim of:
□ enabling stepped operation (modularity),
□ ensuring operation by only the components required;
■ redundancy.

knowing the level of component reliability

The reliability of a system (mechanical, electrical and electronic) is its aptitude to perform a required function, under given conditions, during a given period of time; **it is the probability of system survival** (cf. Cahier Technique n° 144 «Introduction to dependability design»).

As a result, the various mechanical, electrical and electronic constituents must be chosen according to quality and reliability levels, taking into account the thermal, climatic and mechanical environments, this being particularly true for components that bear substantial «weight» on unavailability.

Debugging can be employed to bring out latent defects that are liable to appear in the operating environment, without affecting the quality of the components nor causing wear.

When the components are not certified, qualification bodies can be called in, such as the LCIE for electronics or the ASEFA test stations for electrotechnical components.

The table in figure n° 7 summarizes the main technical choices influencing availability.

choosing technologies

For each constituent (LV switchboard, Generator, «Short-term» back-up), the choice of the various technologies plays a major role in reliability and maintainability.

Low voltage switchboard (LVSB)

Although the equipment comprising the LVSB accounts for only 20 % of system availability, it should be chosen with care.

■ choice between fuses and circuit breakers:
□ fuse: this short-circuit protection device is no longer justifiable at present in dependability installations due to the maintainability constraints it imposes.
□ circuit breaker: apart from customized protection settings, it has a very low MTTR (Mean Time To Repair, actually reclosing time) and should therefore be used whenever a good level of energy availability is required.

■ choice between contactors and remote control circuit breakers:
□ contactor a durable control device; the device is closed when its «coil» is being supplied with power and open when it is not. It is said to be «monostable» (i.e. a single stable position: open),
□ remote control circuit breaker: this device is of the bistable type, i.e. it maintains its closed or open position in the event of a voltage drop.

Circuit breakers are therefore chosen for high availability stations so that the control position prior to power supply or electronics losses will be maintained.

■ protection devices
If only the faulty feeder is isolated by the circuit breaker located immediately upstream from the fault, and if the feeder is isolated by that circuit breaker alone, this being the case for all fault values ranging from overloads to short-circuits, there is said to be «discrimination».

Discrimination contributes to continuity of service, and hence to energy availability.
Choosing the appropriate discrimination technique is therefore of some consequence.
□ amperage level discrimination: this technique utilizes instantaneously operating circuit breakers. The scaling of settings according to short-circuit current values can provide partial or total discrimination;
□ time-based discrimination: this technique involves the scaling of operation times for circuit breakers fitted with tripping devices with adjustable short and long timer settings. Discrimination is total. However the constraints and the destructive effects caused by short circuits during time delays can be considerable and can reduce maintainability;
□ the SELLIM system (cf.« Cahier Technique» n° 126) combines total discrimination requirements with the advantages of strong short-circuit current limitation.

Also to be cited are the Logic Discrimination System used especially in Medium Voltage (cf. «Cahier Technique» n° 2) which provides total discrimination with delay times reduced to a minimum.

■ fixed or withdrawable equipment
A choice needs to be made between fixed circuit breakers that require switchboard de-energizing in order to be changed and withdrawable breakers which can be replaced with the power on.

When choosing a remote control circuit breaker that will have a high rate of operation, it is advisable to select a withdrawable circuit breaker.

It should also be ensured that the system can evolve; for example that the addition of control-monitoring auxiliaries would be possible.
It is important to seek the most suitable balance between equipment cost and MTTR.
For availability levels greater than 10^{-4}, withdrawable equipment is recommended because of the following elements:
withdrawal (base + circuit breaker):
- MTBF = 100 years, MTTR = 1 hour,
- circuit breaker unavailability = $3.4.10^{-6}$
fixed:
- MTBF = 100 years, MTTR = 24 hours,
- circuit breaker unavailability = $2.4.10^{-5}$

Diesel generator set

■ starting system: this is the sensitive point; it can be pneumatic, connected to a compressor, or electric, connected to a rectifier/charger and battery.
The elements involved in choosing between a pneumatic or an electric starter are the following (the choices made are shown in the table in figure n° 7):

□ electric starter:
Advantages:
- simple to supervise,
- simple to install for generators with power ratings < 500 kVA,

levels of unavailability required for the installation as a whole:	10^{-6}	5.10^{-6}	10^{-6}	10^{-4}
type of starter (P > 1MVA)				
electric + pneumatic	■	■		
pneumatic only			■	■
fuel supply				
by the force of gravity (or two pumps)	■	■		
with a single pump			■	■
lubrication circuit (depending on the motor)				
with added oil		■	■	
with prelubrication		■	■	■

fig. 7: choices of technologies for a diesel generator set.

- no effect on motor ageing,
- simple to maintain;
Drawbacks:
- monitoring the starter battery is a delicate matter,
- inoperative when mechanical starter ring positioning faults occur;
- large size for power ratings > 1 MVA,
- installation constraint: the battery must be near the motor; it is often of the maintenance-free type and must be capable of «sudden discharges».

□ pneumatic starter:
Advantages:
- simple to supervise circuit starting,
- lower cost and smaller sizes for generator power ratings > 500 kVA;
Drawbacks:
- supervision of compressor is a delicate matter,
- corrective maintenance can be long and delicate.

■ taking the environment into account
The ambient temperature of the generator as well as altitude can reduce generator performances.
As an example:
□ an ambient temperature of 40 °C will bring about a declassification of 10 % (rated temperature 25 °C),
□ an altitude of 2,000 m will cause a declassification of 25 % (rated at 100 m).
These declassifications are functions that are proportional to the variable and lead to motor oversizing and oversupply.

Too low a motor idling temperature (< 15 °C) can cause the motor to stall when taking on a load. It is possible to remedy this by installing a preheating circuit on the oil and water circuits for water-cooled motors, or on the oil circuit for air-cooled motors.

It is also possible to stagger the resupply of electricity to the circuits, starting with the highest priorities.

«Short-term» back-up (UPS)
This function, fulfilled by an uninterrupted power supply (UPS) largely contributes to the objective of power station availability. Four criteria are to be taken into consideration in establishing the optimal configuration for short-term back-up:
■ power used in normal operation,
■ instantaneous load variations (load side),
■ availability level desired,
■ autonomy required.

The choice of technology includes various elements that enable the UPS to operate properly:
■ supply-side and load-side protection devices,
■ connection cabling,
■ battery supply.

Regarding protection devices, particular attention should be paid to the setting of overcurrent devices (magnetic and thermal circuit breaker trip mechanisms) since:
■ current peaks frequently occur during switch-on,
■ UPS have reduced short-circuit power. It is therefore necessary to check:

$I_{\text{current peaks}} < I_{\text{protection limit}} < I_{sc}$.

As for the equipment for protecting (people) against insulation faults, «unearthed neutral» systems should be chosen whenever possible since there is no tripping when the first fault occurs.

For batteries it is advisable to:
■ choose a technology that facilitates maintenance: lead-sealed battery or maintenance-free lead battery;
■ provide access enabling quick replacement.
The type of operation and short-term back-up configuration should correspond to the level of availability required for the planned application:
■ n° 1: continuous «on line»operation of the UPS is preferable to «off line» operation and is imperative when the UPS protects against micro-cuts.
With «off line» operation, the UPS only supplies power with the mains off.
With «on line» operation, the mains are back-up for the UPS when overcurrent or a static power supply failure occur. The elements supplied by the UPS are then backed up directly by the mains through the static contactor (SC).
■ n° 2: several static power supplies coupled in parallel, with no redundancy and no use of a back-up network; this configuration allows suitable distribution according to the power required by the backed-up equipment, and stepped operation according to static power supply availability.
■ n° 3: several static power supplies coupled in parallel, with redundancy and without the use of a back-up network; this configuration offers greater availability than the two previously described, availability depending directly on the level of redundancy.
■ n° 4: several static power supplies coupled in parallel, one of which is redundant with the use of a back-up network; this configuration offers greater availability than the previous one for a small additional cost.
The table in figure n° 8 gives an indication of MTTF values for different configurations.

configurations	**without a back-up network**	**with a back-up network:**	
		«mains» quality	**good quality**
one static power supply	31,000	183,000	261,000
two static power supplies in parallel wothout redoundancy	15,500	112,000	177,000
two static power supplies in parallel with 1/2 redundancy	250,000	411,000	450,000

fig. 8: MTTF values in hours for different configurations (factory-debugged equipment).

Control-monitoring electronics
The electronics have the role of managing each function in the power station. So as to obtain the greatest possible level of reliability, it is wise to select the following options:
■ high integration level, use of highly integrated components such as microcomputers for the supervision function and a micromonitor for the control-monitoring unit;
■ division of functions at both the control-monitoring and supervision levels, two examples being: on the control unit, separating the interface parts (sensors-actuators) from processing, and on the supervision unit, separating the processing and communication functions;
■ integration of power supplies into their functional levels (e.g. the control unit has its own power supply implanted in its circuit boards);
■ low consumption components;
■ modularity for easy maintainability, if possible without having to interrupt the process.

Sensors and actuators
Special attention should also be paid to the choice of sensors and actuators:
■ for sensors, it is very important to take into account their physical and electrical environments since these are key elements providing:
□ efficient control-monitoring,
□ corrective maintenance assistance,
□ a high level of preventive maintenance;
■ actuators that are directly related to guaranteed power availability must carry out their assignment, regardless of power supply failures or losses of control (problems on the SU or CU). In other words, they must:
□ retain their ON or OFF status (bistable operation),
□ allow operation in manual mode. The circuit breaker is an example.

failure tolerance

If the techniques and technologies chosen are not sufficient to achieve the desired level of availability, failure tolerance can be used. This tolerance is achieved essentially by:
■ redundancy techniques (already referred to regarding short-term back-up),
■ the possibility of stepped operation,
■ the appropriate choice of an earthing system.

Redundancy
Redundancy should be provided for, as a priority, on the equipment that bears the most weight in the calculation of unavailability for the power station as a whole. Let us examine the choices that are possible/and or to be selected.

■ diesel generator set
It is easy to assume that two generators in redundancy will ensure greater availability, but this is true only if the two generators use separate busbars; otherwise availability is decreased by the reliability of the extra coupling device.

■ «short-term» back-up
This level, assigned to supply power to the application during the generator takeover phase, plays an essential role in power station availability. To fulfil the assignment, this level cannot be a common mode.

A practical solution is to divide the risk by the modularity,
□ 3 kW (battery rectifier charger) to supply d.c. feeders such as telecommunication equipment,
□ 3, 40, 80 kVA (UPS) to supply a.c. feeders such as data processing equipment.

This modularity allows:
□ stepped operation, and correction maintenance action without interrupting the power station assignment,
□ power redundancy according to the level of availability required and the repair times imposed by maintenance logistics.

■ low voltage switchboard power source changeover
This is a common mode which, with its control parts, represents a failure rate in the vicinity of 10^{-5}. The following two types of redundancy allow a greater level of availability to be achieved:
□ switchboard redundancy which makes at least 50% of the power distributed by both switchboards available during maintenance,
□ power supply changeover redundancy which is used when an anomaly is detected on the changeover device, taking battery autonomy into account.

■ automation systems
Different types of PLC redundancy can be used. For this type of equipment, we will choose only the following redundancy: two totally asynchronous PLCs that are continuously active in the process, each of them synchronized with process status. The first PLC to enforce an action regarding availability will automatically impose this action on the other PLC. The actuators, by means of their control mechanism cabling, should favour «ON» status. The faulty PLC will withdraw without resetting its watchdog.

■ sensors
Certain measurements, such as speed, temperature, gas oil level, etc. are fundamental to availability, not to mention equipment safety: the sensors used for these measurements are therefore provided with «back-up». The coherency of measurements is assessed by the control-monitoring system in relation to process status and, in the event of an observed incoherence, the system rejects the measurement and declares the sensor to be faulty.

■ power supply for control-monitoring electronics and auxiliaries
So as to enable stepped operation, there should be more than one power source for the various control-monitoring functions in a dependability system. Each function should have its own power supply, and if some of them use the same power supply, it is necessary to provide a protection device for each function.

Earthing systems
The three standard earthing systems or diagrams are the «TT» (earthed), the «TN» (directly earthed neutral) and the «IT» (unearthed) systems.

■ «TT» earthed system
Availability is provided by the choice of residual current circuit breakers with discrimination (amperage level and time-based) which make it possible to

isolate only the faulty feeder and to immediately eliminate the danger without altering installation operation on the whole.

Fault current is limited by the neutral and feeder earth socket impedance and, as a result, faults will not damage the installation.

This system is especially recommended for networks that are liable to be modified, altered by mobile or temporary receivers, or operated by non-specialized personnel.

■ «TN» directly earthly neutral system
In this system, all insulation faults cause short circuits with current greater than the tripping limit of the short-circuit protection device.

Availability depends upon the choice of the discrimination technique and the overcurrent protection devices (cf. chap. 4 §»LVSB technology choices»). It should be noted that the TNS (separate neutral and protective conductor) system, when combined with the use of residual current devices is preferable to the TNC (combined neutral and protective conductor) system in terms of possible installation damage. Waiting for strong fault current to form is synonymous with major damage, particularly in receivers. This has a definite effect on maintainability and hence on availability.

■ «IT» unearthed system
Insulation faults do not entail any risks for people and do not require isolation by disconnection of the faulty portion; hence no breaking takes place.

It is therefore advisable to track the fault and clear it before a second one occurs since if this happens (as in the TN system), one (or both) of the faulty feeder circuit breakers would open.

The current of the first fault is very weak and does not cause any damage. This earthing system should be chosen for the best availability provided that... the first fault is tracked.
With this earthing system, reference can be made to «fault tolerance».

Summary of the choices
The choice of techniques related to failure tolerance according to the level of unavailability are summarized in the table on the next page (cf. fig. 9).

running the installation

The electronics play an active part in the level of dependability by assisting personnel with operation and maintenance tasks, in the aim of compensating for possible failures.

Human behaviour is considered as a failure if it reduces, even partially, the system reliability. The following question must be asked:
«What sort of work sharing is assigned to the Man Machine pair?»

The use of automatic control-monitoring is based on the following criteria:
■ reflex perception, decision and action,
■ complexity and implementation,
■ repetitive procedures.
For example, switching from the main power source to generator power can be assigned to the system.

Human intervention is found at two levels:
■ system control-monitoring (veto regarding functional matters),
■ taking into account of maintenance with system assistance for the user.
Hence:
■ the division of tasks reduces the effect of human errors since people do no intervene in the normal operating process,
■ man is considered as an agent who contributes to reliability by checking and he is the last bastion of safety in the event of system malfunction.
The electronics are broken down into three levels:

accessible unavailability levels for an installation as a whole according to its architecture:		**10^{-6}**	**5.10^{-6}**	**10^{-5}**	**10^{-4}**
redundancy					
of CUs	for the generator	■	■	■	■
	in the LVSB	none	■	■	■
of power source changeovers		■	■	■	none
of sensors (voltage and oil, water, pressure levels...)		■	■	■	none
of UPSs	level/total power	1/6	1/6	1/8	none
	modularity	■	■	■	■
of the generator		none	none	none	none
of specific distribution for electronic devices		■	■	■	■
earthing system		**IT**	**IT**	**TT** or **TNS** or **IT**	**TN** or **TT** or **IT**

It should be note that the generator has no redundancy since the purpose it whould serve does not justify the very high cost it would entail. A reminder regarding erathing systems: **IT** = continuity of service, **TT** = reduced damage when insulation faults occur.

fig. 9: technical choices relatives to failure tolerance.

■ CU for control-monitoring
■ SU for supervision
■ MU (management unit) for global management (cf. fig. 10).

The equipment level has already been discussed at length as well as the control-monitoring (CU) level.
The SU and MU levels, while less operational, are just as important.

Supervision level (SU)
This level provides the user in real time with an indication of process status in the form of:

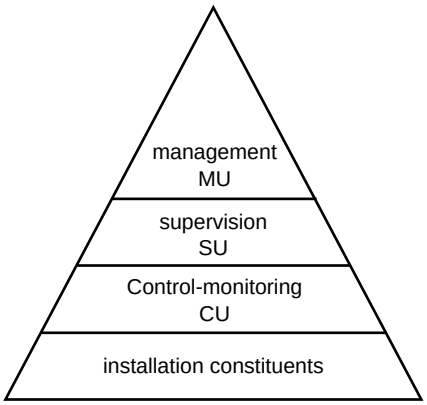


fig. 10: hierarchical levels of electricity technical management.

□ alarms establishing the nature of the fault together with the type of clearance and repair,
□ logs providing access to the history of faults and process status changes,
□ system reports giving process status in real time.

This level also enables the user to perform control-monitoring and hence to intervene in the system by means of the Man Machine Relation (MMR) via an operator terminal in the form of:
□ read-out of system reports,
□ modification of process operating parameters,
□ start of testing,
□ alarm clearance,
□ time changes,
□ etc.

Management level (MU)
When such a level exists, for several stations spread across a geographical area, it is remote from the local system and manages stations with the following functions:
□ remote supervision,
□ inventory,
□ statistics,
□ remote control with interlocking corresponding to the selected levels of availability.

Should a problem occur, the user can be alerted locally by a radio call system. He then connects with the MU that generated the call by means of a telephone equipped for example with a Minitel. Once he is aware of what is happening, he can make the initial arrangements before going to the local control-monitoring station, if necessary.

These different levels take part in:
□ **corrective** maintenance, by enforcing inspection of all repairs on sub-assemblies that are critical to the power availability assignment. Only a positive test result will clear the alarm at the origin of the request for repairs,
□ **preventive** maintenance, by automatically or manually conducting periodic testing according to an electronically controlled schedule.

Communication
(cf. fig. 11)
The reliability of communication (by bus) between the various levels is also very important:
□ it ensures the exchanges between
- installation and CU (by bus if intelligent sensor-actuators are used),
- CU and SU,
- SU and MU.
□ it also enables the user to communicate with the system both locally and remotely.
Operation, management and archiving data can be:
□ unidirectional for file transfers and periodic collection of maintenance information,
□ interactive, of the command/answer type for remote control and remote diagnostic operations.

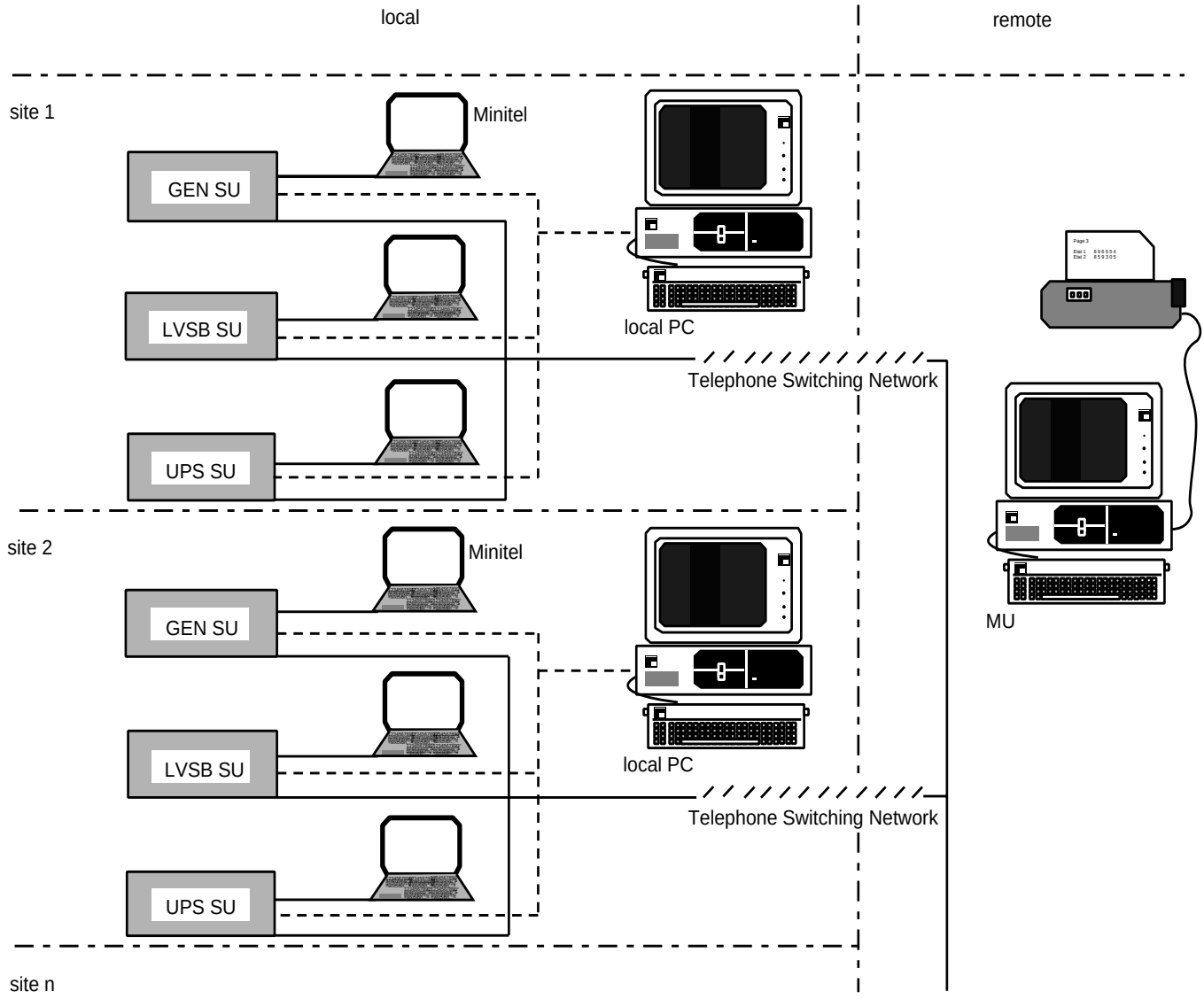


fig. 11: architecture for communication with user.

5. example of increased availability backed-up distribution

specification

Unavailability rate: 10^{-5}, i.e. 6 minutes per year (cf. fig. 12 and 13)
Repair time: 8 h, for the repair of components liable to eventually comprise the assignment. As an image: the time required to repair **the belt when both the belt and suspenders are being used at the same time**.

construction

Based on the diagram in figure 4, the weak points of the installation (cf. chapter 2) should be improved and measures should be taken in terms of maintenance so as to divide the unavailability rate by 60.

Action on installation components

■ diesel generator set
□ motor oversized by 30 % (full power can only be supplied when the motor is cold) or continuous preheating;
□ starting chain composed of:
- an electric starter up to 600 kVA and a pneumatic one thereabove,
- two chargers equipped with a battery,
- two speed measurement chains,
□ gas oil circuit supplying the motor by the force of gravity;
□ lubrication circuit controlled by two temperature measurements;
□ two ventilation circuits;
□ closed circuit water cooling with a lost water cooling circuit as well, connected to the public water system;
□ two control-monitoring units.
■ power source changeover device
The «standby» circuit breaker is backed up by a contactor which intervenes when ordered to do so by the control-monitoring unit (CU) in the event of a power source changeover failure.
■ short-term back-up
The calculation shows that it is necessary to provide a minimum power redundancy of 10 %, implying modular equipment with total power exceeding rated power.

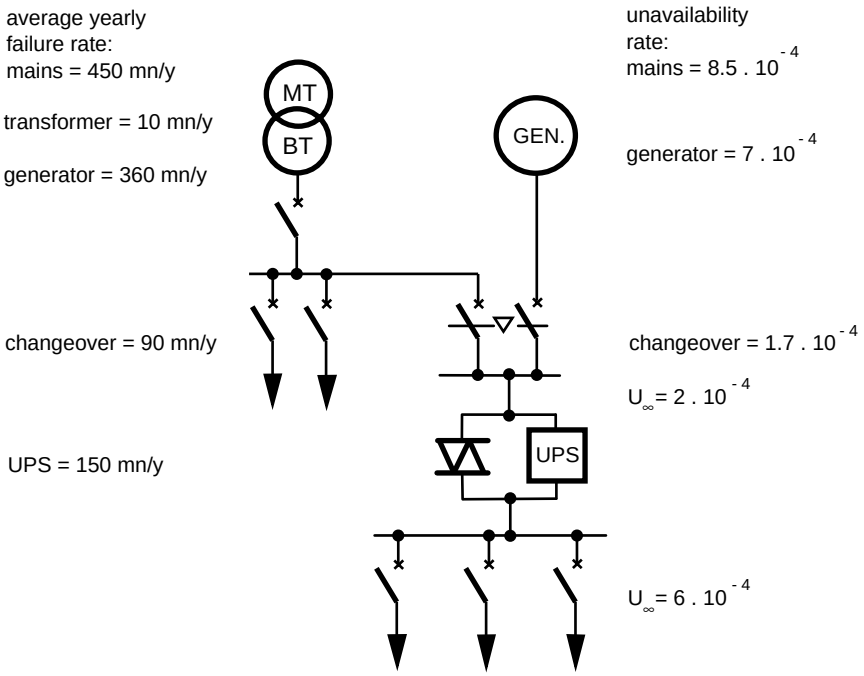


fig. 12: standard equipment produces an unavailability rate of 5h/y.

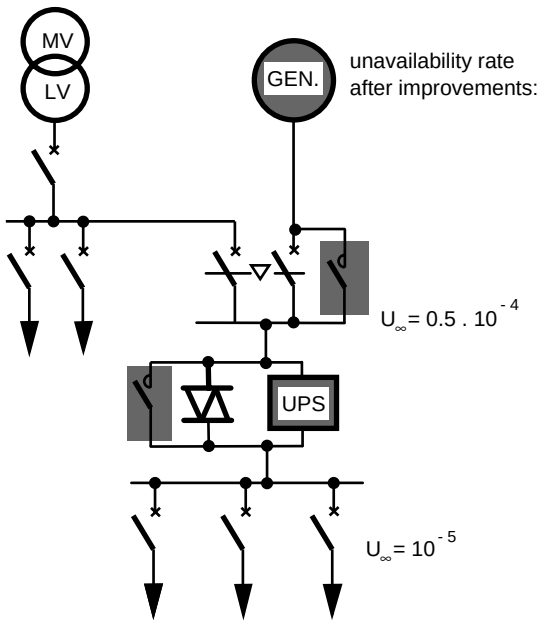


fig. 13: the inprovement of sensitive points (GEN - M/S and UPS) enables feeders to attain unavailability rates of 6 mn/y.

maintenance arrangements

■ electronics: a circuit board of each type for SU and CU.
■ power: a sub-assembly corresponding to each element that is critical to the performance of the assignment, throughout the chain, and which takes part in power supply to feeders with increased availability.

Composition of the maintenance package:
■ preventive maintenance
Action is requested by the system following either periodic testing or time-delayed alarms related to the end of operating intervals (e.g. generator discharge). In this case, the user should take action within 48 hours of the time the alarm is generated.
■ corrective maintenance
This refers to repair action taken as a result of alarm generation.
All measures should be taken to ensure quick repair. The 10^{-5} rate corresponds to the proper operation time before the first repair and proceeds from preventive maintenance.
If, through negligence, the high availability power supply should enter the corrective maintenance system, the unavailability rate will drop. The mean time to repair will then be added on to the 6 minutes.
The composition of the maintenance package and the efficiency of the maintenance department will therefore be determining factors.

demonstrating specified availability

The detailed calculation is far too complicated to be presented here.
By simplifying to a large extent, based on the data in figure n° 12:
■ the probability of a voltage drop in the main LV circuit breaker is 450 mn/y, i.e. $U_{\infty} = 10^{-3}$,
■ the probability of a voltage drop downstream from the power source changeover corresponds to the probability of the simultaneous occurrence of a mains failure and
□ the generator out of operation after 5 minutes' time,
or

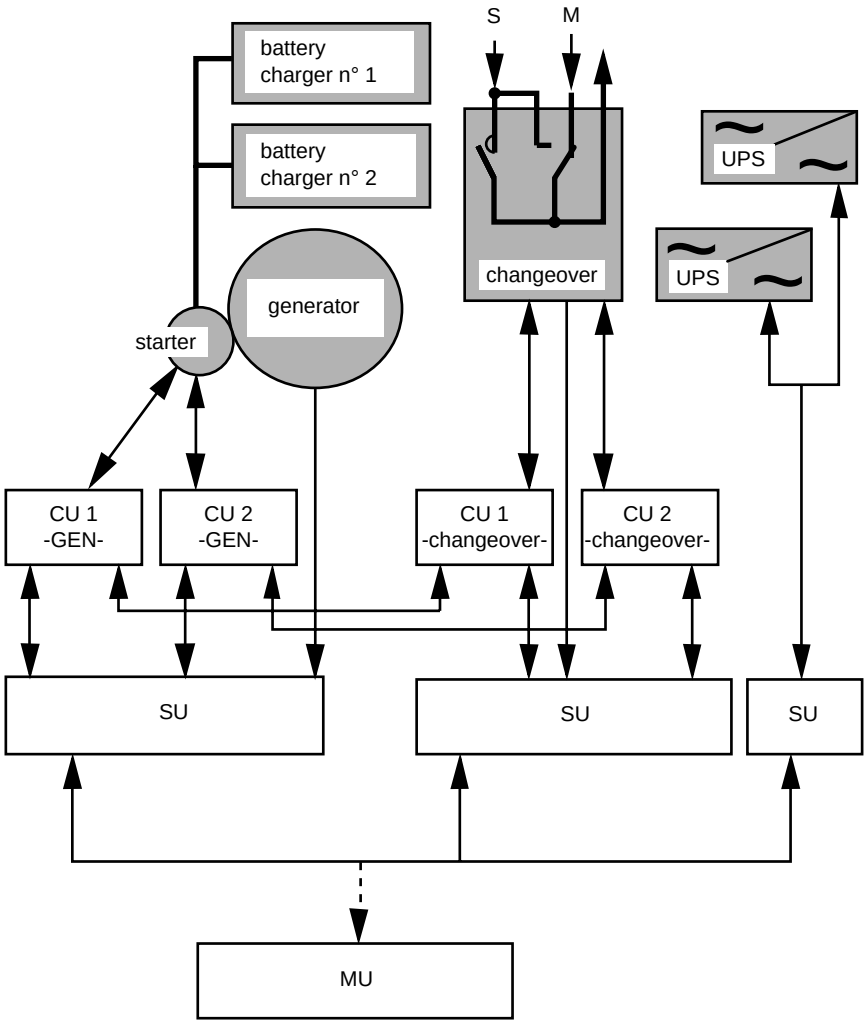


fig. 14: control-monitoring corresponding to unavailability of 10^{-5} (6 mn/y).

□ the power source changeover out of service.
This probability is very close to the changeover failure rate which is a common mode (compulsory stage), i.e. in the range of 100 mn/y, equivalent to $U_{\infty} = 2.10^{-4}$.
Backing up the changeover by a contactor will raise this rate to $0.5.10^{-4}$.
The probability of a voltage drop at the feeder level reaches 10^{-5} with the UPS and static contactor which prevent micro-cuts, backed up by an electromagnetic contactor.

Referring to the table in figure n° 8, this solution corresponds to an MTTF of 261,000 h, taking repair time into account.
The MTBF for the installation as a whole is therefore in the range of 100,000 h, i.e. an average unavailability rate of 6 minutes per year.

6. conclusion

The spread of process technical management, building utilities and electrical power distribution entails continuous power supply for those systems, at the control-monitoring level and, to an increasing extent, at the power level.
Mastering energy availability is nowadays a necessity for electricians.

This «Cahier Technique» shows that this objective can be achieved, provided that:
■ a global approach is used, including the establishment of:
□ objectives (needs),
□ operating criteria,
□ conditions of use,
(training, supervision, maintenance):
■ and action is taken regarding:
□ component reliability,
□ fault tolerance,
□ component redundancy,
and, naturally:
□ information processing,
in other words: control-monitoring intelligence.

We have seen that to improve availability, efforts must be focused essentially on:
■ back-up sources close to the feeder,
■ common mode (compulsory path) equipment circuits,
■ preventive maintenance.

It is currently possible to attain unavailability rates of 10^{-6} (less than a minute per year) thanks to UPS in particular, for power ratings that can reach several hundreds of kW.
With power UPSs, the concept of **clean, dependable mains** has emerged.

7. bibliography

Publications

■ Un nouveau système d'alimentation à haute disponibilité (A new high availability power supply system).
C. Francon and R. Delooze
Merlin Gerin.
SEE Conference.

■ The decentralized DC unit in telecommunications equipment energy systems.
J.P. Leblanc and D. Marquet, CNET,
G. Gatine, Merlin Gerin
INTELLEC 1987 Conference.

■ The operation of the GEODE energy system.
J.P. Leblanc and D. Marquet, CNET.
J.M. Rollet, Merlin Gerin.
INTELLEC 1986 Conference.

■ A new material and data processing design for the availability target: the GEODE system.
J.C. Chigolet, CNET,
M.J. Gérard Seri, Renault,
C. Franco, Merlin Gerin.
INTELLEC 1985 Conference.

Merlin Gerin's «Cahiers Techniques»

■ Protection of electrical distribution networks by the logic selectivity system
Cahier Technique n° 2
(R. Calvas - F. Sautriau)

■ La sélectivité des protections
Cahier Technique n° 13
(F. Sautriau)

■ Low voltage protection system selectivity: SELLIM system
Cahier Technique n° 126
(C. Albertin)

■ Industrial approach dependability
Cahier Technique n° 134
(H. Krotoff)

■ Introduction to dependability design
Cahier Technique n° 144
(P. Bonnefoi)

Réal. : Illustration Technique - Photo : IPV
IPV - 10/91 - 2500 - Imprimeur : Léostic